CLAIM AMENDMENTS

This listing of claims will replace all prior versions, and listings, of claims in the application.

| 1 | 1. (currently amended) A method of configuring a network security system, |
|----|--|
| 2 | comprising: |
| 3 | a. forming a registry data structure for defining roles within a |
| 4 | network; |
| 5 | b. mapping network security policies to the registry data structure, |
| 6 | said network security policies being contained in one or more policy |
| 7 | documents, the one or more policy documents being in a standard document |
| 8 | format language and being stored in machine readable form; and |
| 9 | c. using a document transformation algorithm to transform the |
| 10 | policy documents into one or more device-specific configuration documents |
| 11 | stored in machine-readable form. |
| 1 | 2. (original) The method according to claim 1, further comprising generating |
| 2 | instances of the roles and associated security policies, each instance being |
| 3 | mapped to physical segments of the network. |
| 1 | 3. (original) The method according to claim 1, further comprising distributing |
| 2 | the device-specific configuration documents to network entities for |
| 3 | implementing the network security policies. |
| 1 | 4. (original) The method according to claim 1, wherein the registry data |
| 2 | structure comprises a collection of documents that include information |
| 3 | regarding the network roles and topology of the network. |
| 1 | 5. (original) The method according to claim 1, wherein the registry data |
| 2 | structure comprises a hierarchy of network types, each type comprising a |
| 3 | definition of a network role. |

1 6. (original) The method according to claim 5, wherein each network role is 2 representative of a set of applications to be supported by the network. 1 7. (original) The method according to claim 5, wherein when a parent 2 network type is mapped to a policy contained in one of the policy documents, 3 a child network type of the parent network type inherits the policy. 1 8. (currently amended) The method according to claim 7, wherein when the child network type is mapped to a policy contained in one of the policy 2 3 documents that is in conflict with the policy inherited from the parent, the policy mapped to the child takes precedence over the policy inherited from the 4 5 parent. 1 9. (original) The method according to claim 5, wherein an instance of one of 2 the network types is mapped to one or more physical network segments and 3 wherein the network type includes a set of data fields for defining the physical 4 network segments. 1 10. (currently amended) The method according to claim 6, wherein at least 2 one of the network types is an abstract type without an instance mapped to a 3 physical network segment. 1 11. (original) The method according to claim 5, wherein each network type 2 further comprises a data field for identifying a human administrator. 1 12. (original) The method according to claim 5, wherein each network type 2 further comprises a data field for providing a human readable description of 3 the network type. 1 13. (original) The method according to claim 1, wherein the network security 2 policies are representative of restrictions to be placed on one or more of the 3 network roles in the registry data structure.

| 1 | 14. (original) The method according to claim 1, wherein the policy |
|----|--|
| 2 | documents are in extensible markup language (XML). |
| 1 | 15. (original) The method according to claim 1, wherein the document |
| 2 | transformation algorithm is specific to a network entity utilized for |
| 3 | implementing one or more of the security policies contained in the policy |
| 4 | documents. |
| 1 | 16. (original) The method according to claim 15, wherein the document |
| 2 | transformation algorithm includes style sheet language for transformation |
| 3 | (XSLT) controlled by a script. |
| 1 | 17. (original) The method according to claim 16, wherein the script is |
| 2 | specific to a network entity. |
| 1 | 18. (original) The method according to claim 16, further comprising a step of |
| 2 | selecting the script from among a plurality of scripts, each being specific to a |
| 3 | different network entity. |
| 1 | 19. (original) The method according to claim 16, wherein the device-specific |
| 2 | configuration documents are in plain text format. |
| 1 | 20. (currently amended) A apparatus for configuring a network security |
| 2 | system, comprising: |
| 3 | a. a registry data structure including a plurality of network types, |
| 4 | each network type being stored within a document in the registry and |
| 5 | including a role definition and a set of fields defining segments of a network; |
| 6 | b. security policy documents mapped to the registry data |
| 7 | structure, each security policy document being in a standard document format |
| 8 | language and being representative of restrictions to be placed on a network |
| 9 | type in the registry data structure; and |
| 10 | c. a document transformation algorithm for transforming the |
| 11 | documents in the registry and the policy documents into device-specific |
| 12 | configuration documents stored in machine-readable form. |